

CLAIM AMENDMENTS

This listing of claims will replace all prior versions and listings of claims in the application.

1 1. (Currently Amended) A processor ~~for encrypting and decrypting that performs an~~
2 encryption/decryption operation data, the processor comprising:

3 a control device that receives ~~a data word for encryption or decryption at~~
4 least one initial key, the control device comprising:

5 a memory that temporarily stores ~~an~~ the at least one initial key, and

6 at least one external key input that receives the at least one initial key

7 from a source;

8 a round key generator connected to the control device via at least one further
9 communication device, wherein the round key generator receives the ~~data word at~~

10 least one initial key from the control device ~~for calculating to calculate~~ at least one

11 round key and transfers the at least one round key to the memory of the control

12 device; ~~and~~

13 at least one encryption/decryption device comprising:

14 at least one external data input that receives external data,

15 an input that receives the at least one round key from the memory of

16 the control device, and

17 at least one external data output that outputs data processed with the
18 at least one round key, wherein the at least one encryption/decryption device
19 and the round key generator communicate solely via the control device, and
20 the control device transmits intermediate results to the round key generator
21 to perform recursive calculation of the at least one round key;

22 a first request line that sends requests from the at least one
23 encryption/decryption device to the control device; and

24 a second request line that sends requests from the round key generator to the
25 control device, wherein the at least one encryption/decryption device and the round
26 key generator both transmit requests on the respective first and second request
27 lines to start the encryption/decryption operation after both requests are met.

1
2 2. (Currently Amended) The processor of claim 1, wherein the at least one
3 communication device further comprises:

4 ~~first and second request lines;~~

5 first and second release lines; and

6 first and second data lines.

1 3. (Previously Presented) The processor of claim 2, wherein the first and second
2 request lines, the first and second release lines, and the first and second data lines
3 at least partially use a single physical path.

1
1 4. (Previously Presented) The processor of claim 1, wherein the at least one round
2 key is temporarily stored in the memory of the control device.

1
1 5. (Previously Presented) The processor of claim 1, wherein the at least one round
2 key is accessed using a rotating pointer.

1
1 6. (Previously Presented) The processor of claim 1, wherein the communication
2 between the control device and the at least one encryption/decryption device and
3 between the control device and the round key generator is accomplished using at
4 least one handshake protocol.

1
1 7. (Previously Presented) The processor of claim 1, wherein the operation of the
2 control device, of the at least one encryption/decryption device, and of the round key
3 generator are asynchronous with respect to one another.

1 8. (Currently Amended) The processor of claim 1, wherein the round key generator
2 ~~is adapted to perform~~ performs a dummy operation.

1 9. (Previously Presented) The processor of claim 1, wherein a time between the
2 calculating of the at least one round key by the round key generator and the
3 processing of the external data using the at least one round key is variable.

1 10. (Previously Presented) The processor of claim 1, wherein the processor is an
2 Advanced Encryption Standard (AES) coprocessor.

1 11. (Currently Amended) A method of ~~encrypting and/or decrypting~~ data
2 performing an encryption/decryption operation using a processor, the method
3 comprising:

4 sending a first request on a first request line from at least one
5 encryption/decryption device to a control device and a second request on a second
6 request line from a round key generator to the control device to start the
7 encryption/decryption operation after both requests are met;

8 reading at least one initial key into ~~a~~ the control device, wherein the at least
9 one initial key is obtained from a source other than ~~a~~ the round key generator;

10 reading external data into the at least one encryption/decryption device;

11 reading at least one data word needed to calculate at least one round key
12 from at least one storage device of the control device;

13 transferring the at least one data word to the round key generator;

14 calculating at least one round key recursively on the basis of the at least one
15 data word by using the round key generator;

16 transferring the ~~calculated~~ at least one round key to the control device; and
17 storing the ~~transferred~~ at least one round key in the at least one storage
18 device;

19 transferring the at least one round key from the at least one storage device to
20 the at least one encryption/decryption device;

21 processing the external data by using the at least one encryption/decryption
22 device, using the at least one round key, and ~~using~~ the processed data are made
23 available at at least one external data output; and

24 repeating the method as often as necessary to encrypt or decrypt a set of
25 external data,

26 wherein the control device transmits intermediate results to the round key
27 generator to perform recursive calculation of the at least one round key.

1
1 12. (Previously Presented) The method of claim 11, wherein communication
2 between the control device and the at least one encryption/decryption device, and

3 between the control device and the round key generator is accomplished using at
4 least one handshake protocol.

1
1 13. (Previously Presented) The method of claim 11, wherein the operation of the
2 control device, of the at least one encryption/decryption device, and of the round key
3 generator are asynchronous with respect to one another.

1
1 14. (Previously Presented) The method of claim 11, wherein the at least one round
2 key is accessed using a rotating pointer.

1
1 15. (Previously Presented) The method of claim 11, further comprising:
2 performing a dummy operation using the round key generator.

1
1 16. (Currently Amended) The method of claim 11, wherein a time between the
2 calculating of the at least one round key by the round key generator and the
3 processing of the external data using the at least one round key is variable.

1
1 17. (Previously Presented) The method of claim 11, wherein the processor is an
2 Advanced Encryption Standard (AES) coprocessor.